ABSTRACT OF THE DISCLOSURE

An encryption processing apparatus and method in which the difficulty of encryption analysis based on power analysis can be increased considerably are provided. By dividing an original encryption processing sequence into a plurality of groups and by mixing the processing sequence by setting dummies as necessary, several hundreds to several thousands of types of different mixed encryption processing sequences can be set, and a sequence selected from a large number of these settable sequences is performed. According to this configuration, consumption power variations which are completely different from consumption power variations caused by a regular process possessed by the original encryption processing sequence can be generated, and thus the difficulty of encryption analysis based on power analysis can be increased considerably.